



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2000347942 A**(43) Date of publication of application: **15.12.00**

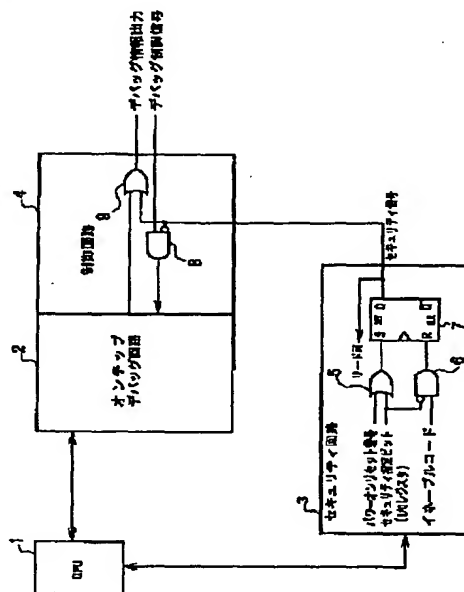
(51) Int. Cl.

**G06F 12/14****G06F 11/22****G06F 15/78**(21) Application number: **11158256**(22) Date of filing: **04.06.99**(71) Applicant: **TOSHIBA CORP**(72) Inventor: **TANABE TETSUYA  
ASAI EIICHI****(54) INFORMATION PROCESSOR****(57) Abstract:**

**PROBLEM TO BE SOLVED:** To protect information stored in a ROM from an illegal access caused by a debug tool provided externally.

**SOLUTION:** An on-chip debug circuit 2 mounted in the information processor is made invalid by power-on reset, and an on-chip debug ICE (in-circuit emulator) is prohibited from accessing an incorporated ROM. The invalidation of the circuit 2 is released by setting an I/O register released to a user by a user program.

COPYRIGHT: (C)2000,JPO



1

(19)日本国特許庁 (J P)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開2000-347942

(P 2 0 0 0 - 3 4 7 9 4 2 A)

(43)公開日 平成12年12月15日(2000.12.15)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テマコード (参考)
G06F 12/14	310	G06F 12/14	310 E 5B017
11/22	340	11/22	340 A 5B048
15/78	510	15/78	510 C 5B062

審査請求 未請求 請求項の数 5 O L (全 8 頁)

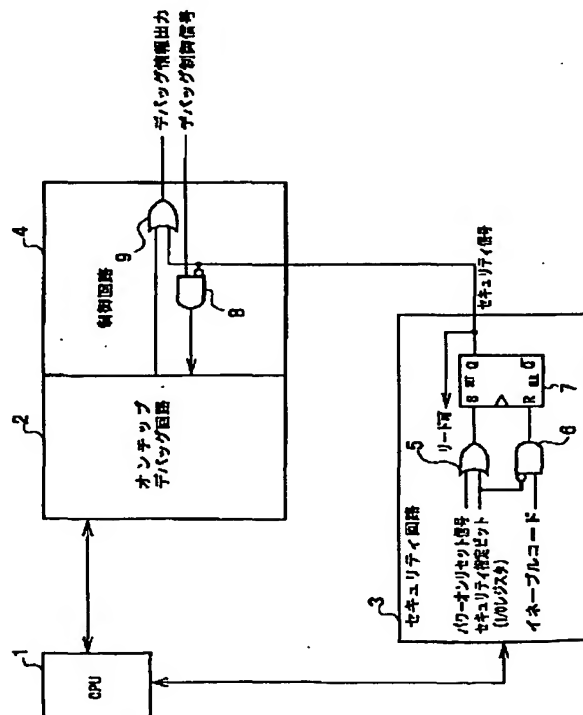
(21)出願番号	特願平11-158256	(71)出願人	000003078 株式会社東芝 神奈川県川崎市幸区堀川町72番地
(22)出願日	平成11年 6 月 4 日(1999.6.4)	(72)発明者	田部 徹也 神奈川県川崎市幸区小向東芝町 1 番地 株 式会社東芝マイクロエレクトロニクスセン ター内
		(72)発明者	浅井 栄一 神奈川県川崎市幸区小向東芝町 1 番地 株 式会社東芝マイクロエレクトロニクスセン ター内
		(74)代理人	100083806 弁理士 三好 秀和 (外 7 名) 最終頁に続く

(54)【発明の名称】 情報処理装置

(57)【要約】

【課題】 この発明は、ROMに記憶された情報を、外部に設けられたデバッグツールによる不正アクセスから保護することを課題とする。

【解決手段】 この発明は、情報処理装置内に実装されているオンチップデバッグ回路2をパワーオンリセットにより無効化し、オンチップデバッグICEによる内蔵ROMのアクセスを禁止し、オンチップデバッグ回路の無効化は、ユーザプログラムによりユーザに開放されたI/Oレジスタの設定により解除されるように構成される。



メモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力制御を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化してセキュリティを設定し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、セキュリティ指定ビットと、このセキュリティ指定ビットのリセットをイネーブルとするイネーブルコードとを受けて、前記オンチップデバッグ回路の機能を有効化してセキュリティを解除し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする。

【0007】第2の手段は、前記第1の手段において、前記セキュリティ指定ビットは、電源投入時にセットされて前記オンチップデバッグ回路の機能が無効化されセキュリティが設定されている状態、又は前記ROMに記憶されたセキュリティ解除プログラムによりリセットされて前記オンチップデバッグ回路の機能が有効化されセキュリティが解除されている状態を有することを特徴とする。

【0008】第3の手段は、前記第1の手段において、前記セキュリティ回路は、前記オンチップデバッグ回路を無効化する際に、一部機能を有効化してなることを特徴とする。

【0009】第4の手段は、外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、電源投入時に前記情報処理装置をリセットするパワーオンリセット信号を受けて、前記オンチップデバッグ回路の機能を無効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを禁止し、予め登録されたコードと外部から与えられたパスワードとを照合して両者が一致した場合には、前記オンチップデバッグ回路の機能を有効化し、前記エミュレータによる前記メモリの記憶情報の読み出しを可能にするセキュリティ回路とを有することを特徴とする。

【0010】第5の手段は、外部に設けられたエミュレータによる不正アクセスから記憶情報を保護するメモリと、前記エミュレータに接続されて、前記エミュレータと情報処理装置との間でデバッグに必要な信号の入出力を行い、前記情報処理装置のデバッグをサポートするオンチップデバッグ回路と、前記エミュレータから暗号化されて前記情報処理装置に与えられるデバッグに必要な信号を復号化し、前記情報処理装置のデバッグ結果を暗号化して前記エミュレータに出力する暗号化回路とを有することを特徴とする。

【0011】

【発明の実施の形態】以下、図面を用いて本発明の実施形態を説明する。

【0012】図1はこの発明の一実施形態に係る情報処理装置の要部構成を示す図であり、図2はデバッグの手順を示すフローチャートである。

【0013】図1において、この実施形態の情報処理装置のマイコンは、CPU1、図示しないROMや周辺回路に加えて、前述したと同様のオンチップデバッグ回路2、セキュリティ回路3、制御回路4を備えて構成されている。

【0014】セキュリティ回路3は、電源投入時にマイコンをリセットするパワーオンリセット信号とセキュリティ指定ビットを入力とする論理和（OR）ゲート5と、セキュリティ指定ビットの反転とセキュリティ指定ビットのリセットをイネーブルとするイネーブルコードを入力とする論理積（AND）ゲート6と、ORゲート5の出力をセット（S）入力としANDゲート6の出力をリセット（R）入力とし出力（Q）をセキュリティ信号として制御回路4に与えるレジスタ（RSフリップフロップ）7を備え、パワーオンリセット信号を受けてオンチップデバッグ回路2の機能を無効化してセキュリティを設定し、エミュレータによるメモリの記憶情報の読み出し、特にオンチップデバッグICE（インサーキットエミュレータ）によるROMの記憶情報の読み出しを禁止し、リセットされたセキュリティ指定ビットかつイネーブルコードを受けて、オンチップデバッグ回路2の機能を有効化してセキュリティを解除し、オンチップデバッグICEによるROMの記憶情報の読み出しを可能にする。

【0015】制御回路4は、セキュリティ回路3から与えられるセキュリティ信号の反転と、オンチップデバッグICEから与えられてマイコンをデバッグするのに必要となる信号のデバッグ制御信号を入力するANDゲート8と、セキュリティ信号とオンチップデバッグ回路2から与えられるデバッグ結果を入力としデバッグ情報出力をオンチップデバッグICEに出力するORゲート9を備え、セキュリティ信号がセキュリティ回路3から与えられてセキュリティが設定されている場合には、デバッグ制御信号の入力ならびにデバッグ情報の出力を禁止する。

【0016】次に、この実施形態では、以下のような方式でマイコン内のオンチップデバッグ回路2の動作を制御する。

【0017】セキュリティ用のセキュリティ指定ビットをI/Oレジスタに設ける。このセキュリティ指定ビットは、パワーオン時に“1”（セキュリティ有効）にセットされ、オンチップデバッグ回路2は、パワーオンリセットによってオンチップデバッグ回路2の機能が無効となるように初期化される。外部に接続されるオンチッ

オンリセットを利用することにより、一度セキュリティが解除された後は、マイコンの電源を落とすまで、制限無くオンチップデバッグICEを使用できる。

【0028】次に、この発明の他の実施形態について説明する。

【0029】この実施形態の特徴とするところは、上記実施形態のセキュリティ解除判定ルーチンにおいて、予めマイコン内に設定したコードと、外部入力やオンチップデバッグICEからの入力を比較して判定するパスワード方式としてセキュリティの解除プログラムを作成せず、図1に示すセキュリティ回路3に代えて、パワーオンリセット信号によりオンチップデバッグ回路2の機能を無効化し、オンチップデバッグICEによるROMの記憶情報の読み出しを禁止し、予め登録されたコードと外部から与えられたパスワードを照合して両者が一致した場合には、オンチップデバッグ回路2の機能を有効化し、オンチップデバッグICEによるROMの記憶情報の読み出しを可能にする、パスワード判定回路を含むセキュリティ解除回路を組み込む構成を採用したことにある。このような実施形態にあっても、上記実施形態と同様な効果を得ることができる。

【0030】次に、この発明の他の実施形態について説明する。

【0031】この実施形態の特徴とするところは、前述した図1に示す実施形態でのセキュリティ有効時に、オンチップデバッグ機能のすべてを禁止するのではなく、一部のデバッグ機能を許可する、例えばユーザアプリケーションにおいて使用するデバッグ機能があれば、その部分のみ常時許可するようにしたことにある。

【0032】一方、オンチップデバッグICEから暗号化されて情報処理装置に与えられるデバッグに必要な信号を復号化し、情報処理装置のデバッグ結果を暗号化してオンチップデバッグICEに出力する暗号化回路を設け、セキュリティ有効時に、デバッグ情報を暗号化してオンチップデバッグICEへ出力し、オンチップデバッ

グICE側でその暗号の解読を制御し、正規ユーザーのみ暗号を解読してデバッグできるようにしてもよい。このような実施形態にあっても、上記実施形態と同様な効果を得ることができる。

【0033】

【発明の効果】以上説明したように、この発明によれば、パワーオンリセットにより情報処理装置内に実装されているオンチップデバッグ回路を無効化しセキュリティを設定し、オンチップデバッグICEによる内蔵ROMのアクセスを禁止し、ユーザプログラムにより設定制御されるセキュリティ指定ビットに基づいてセキュリティが解除されるようにしたので、ROMに記憶された情報を、外部に設けられたデバッグツールによる不正アクセスから保護することが可能となる。また、セキュリティの解除方法は、ユーザが自由に設定できるため、セキュリティの解除方法が無限となり、守秘性が高くなる。さらに、セキュリティの制御にパワーオンリセットを利用することにより、一度セキュリティが解除された後は、電源がオフされるまでオンチップデバッグICEを制限なく使用することができる。

【図面の簡単な説明】

【図1】この発明の一実施形態に係る情報処理装置の要部構成を示す図である。

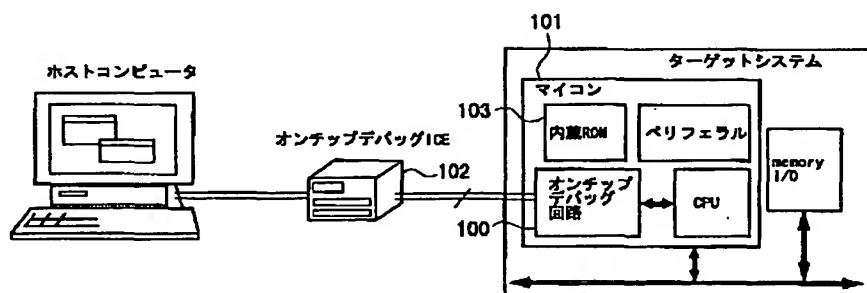
【図2】図1に示す実施形態の動作手順を示すフローチャートである。

【図3】ターゲットシステムをデバッグする従来のシステムを示す図である。

【符号の説明】

- 1 CPU
- 2 オンチップデバッグ回路
- 3 セキュリティ回路
- 4 制御回路
- 5, 6, 8, 9 論理ゲート
- 7 レジスタ

【図3】



【図2】

